



Defense Information Systems Agency  
Joint Information & Engineering Organization  
Center for Information Technology Standards  
<http://www-pki.itsi.disa.mil/>

14 April 2000

## Online Certificate Status Protocol (OCSP) Profile Template

Ref.:

RFC 2279	UTF-8, a transformation format of ISO 10646
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
X.509	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework

## Protocol

Protocol Action	Status	Notes
<b>OCSP Server</b>		
CAs shall include the AuthorityInfoAccess extension in certificates that are to be checked using OCSP.	M	[RFC 2459: 4.2.2.1] [RFC 2560: 3.1]
CAs that support an OCSP service must provide for the inclusion of a value for a uniformResourceIndicator (URI) accessLocation and the OID value id-ad-ocsp for the accessMethod in the AccessDescription SEQUENCE.	M	[RFC 2560: 3.1]
The value of the accessLocation field in the subject certificate defines the transport (e.g. HTTP) used to access the OCSP responder.	M	[RFC 2560: 3.1]
The value of the accessLocation field in the subject certificate may contain other transport dependent information (e.g. a URL).	O	[RFC 2560: 3.1]
The delegated OCSP responder's signing certificate shall include id-kp-OCSPSigning in an extendedKeyUsage certificate extension.	M	id-kp-OCSPSigning      OID ::= {id-kp 9} [RFC 2560: 4.2.2.2]
A CA may specify a responder can be trusted for the lifetime of the responder's certificate.	O	[RFC 2560: 4.2.2.2.1]
The extension id-pkix-ocsp-nocheck is included in the responder's certificate.	m	id-pkix-ocsp-nocheck      OID ::= {id-pkix-ocsp 5} [RFC 2560: 4.2.2.2.1]
This should be a non-critical extension.	o	[RFC 2560: 4.2.2.2.1]
The value of the extension should be NULL.	o	[RFC 2560: 4.2.2.2.1]

Protocol Action	Status	Notes
CAs may issue this certificate with a very short lifetime and renew it frequently.	o/r	A compromise of the responder's key is as serious as the compromise of a CA key used to sign CRLs. [RFC 2560: 4.2.2.2.1]
A CA may specify how the responder's certificate is checked for revocation.	O	[RFC 2560: 4.2.2.2.1]
CRL Distribution Points can be provided if the check should be done using CRLs or CRL Distribution Points.	o	[RFC 2459: 4.2.1.14; RFC 2560: 4.2.2.2.1]
Authority Information Access can be provided to access CA on-line validation services (excluding CRLs).	o	[RFC 2459: 4.2.2.1; RFC 2560: 4.2.2.2.1]
A CA may choose not to specify any method of revocation checking for the responder's certificate.	O	[RFC 2560: 4.2.2.2.1]

OCSP Client		
Systems or applications that rely on OCSP responses must be capable of detecting and enforcing use of the id-ad-ocspSigning value.	M	[RFC 2560: 4.2.2.2]
Applications that receive certificates with other transport dependent information contained in the accessLocation field must be able to process this information	M	
At the OCSP client, the accessLocation for the one or more OCSP signing authorities may be configured, and the set of CAs for which each signing authority is trusted specified.	O	[RFC 2560: 3.1, 4.2.2.2]
<p>Prior to accepting a signed response as valid, OCSP clients shall confirm that:</p> <ol style="list-style-type: none"> <li>1. The certificate identified in a received response corresponds to that which was requested</li> <li>2. The signature on the response is valid</li> <li>3. The identity of the signer matches the intended recipient of the request</li> <li>4. The signer is currently authorized to sign the response</li> <li>5. The time at which the status being indicated is known to be correct (thisUpdate) is sufficiently recent</li> <li>6. When provided, the time at or before which newer information will be available about the status of the certificate (nextUpdate) is greater than the current time</li> </ol>	M	[RFC 2560: 3.2]
<p>If the certificate validating the signature on the response fails to meet at least one of the following criteria, the confirmation that the signer is authorized to sign fails and the response is rejected:</p> <ol style="list-style-type: none"> <li>1. Matches a local configuration of OCSP signing authority for the certificate in question; or</li> <li>2. Is the certificate of the CA that issued the certificate in question; or</li> <li>3. Includes a value of id-ad-ocspSigning in an ExtendedKeyUsage extension and is issued by the CA that issued the certificate in question."</li> </ol>	M	[RFC 2560: 4.2.2.2]

Protocol Action	Status	Notes
The client may apply additional acceptance or rejection criteria either to the response or to the certificate used to validate the signature on the response.	O	[RFC 2560: 4.2.2.2]
If an internalError error message is returned, the OCSP requestor should retry, potentially with another OCSP responder.	O/R	[RFC 2560: 2.3]
OCSP clients shall be capable of receiving and processing responses of the id-pkix-ocsp-basic response type.	M	[RFC 2560: 4.2.1, 4.4.3]
The client is to interpret the thisUpdate and nextUpdate fields as defining a recommended validity interval.	M	[RFC 2560: 4.2.2.1]
Responses whose nextUpdate value is earlier than the local system time value should be considered unreliable.	O/R	[RFC 2560: 4.2.2.1]
Responses whose thisUpdate time is later than the local system time should be considered unreliable.	O/R	[RFC 2560: 4.2.2.1]
OCSP clients must check that an authorized responder's certificate has not been revoked.	M	[RFC 2560: 4.2.2.2.1]
Applications that receive certificates indicating that the responder should be trusted for the responder's certificate lifetime must be able process the certificate according to local policy.	M	
If the responder's certificate includes the extension id-pkix-ocsp-nocheck an OCSP client may trust a responder for the lifetime of the certificate.	O	[RFC 2560: 4.2.2.2.1]
The OCSP client must indicate its support by including the id-pkix-ocsp-nocheck OID in the AcceptableResponses SEQUENCE.	m	[RFC 2560: 4.4.3]
Applications that receive certificates specifying how the responder's certificate is checked for revocation must be able to use the revocation method specified.	M	
If the CA does not specify any method of revocation checking for the responder's certificate, the OCSP client must follow it's local security policy on whether that certificate should be checked for revocation.	M	[RFC 2560: 4.2.2.2.1]
Clients shall be capable of processing responses signed using DSA keys identified by the DSA sig-alg-oid.	M	[RFC2459: 7.2.2; RFC 2560: 4.3]
Clients should also be capable of processing RSA signatures.	O	[RFC2459: 7.2.1; RFC 2560: 4.3]
OCSP client MAY wish to specify the kinds of response types it understands.	O	[RFC 2560: 4.4.3]
OCSP client SHOULD use an extension with the OID id-pkix-ocsp-response, and the value AcceptableResponses.	o/r	The OIDs included in AcceptableResponses are the OIDs of the various response types this client can accept. id-pkix-ocsp-response OID ::= { id-pkix-ocsp 4 } [RFC 2560: 4.4.3]
This extension is included as one of the requestExtensions in requests.	m	[RFC 2560: 4.4.3]

Protocol Action	Status	Notes
The OCSP client may indicate its support of nonce cryptographic binding a request and a response by including OID id-pkix-ocsp-nonce in the AcceptableResponses SEQUENCE, while the extnValue is the value of the nonce.	o	id-pkix-ocsp-nonce OID ::= { id-pkix-ocsp 2 } [RFC 2560: 4.4.1]
The OCSP client may indicate its support for CRL references by including the id-pkix-ocsp-crl OID in the AcceptableResponses SEQUENCE.	o	[RFC 2560: 4.4.2]
An OCSP archive cutoff date is used to prove digital signature reliability as of the date it was produced. Even if the certificate validating the signature has expired.	M	[RFC 2560: 4.4.4]

OCSP Request		
An OCSP request will contain: 1. protocol version 2. service request 3. target certificate identifier	M	Requests do not contain the responder they are directed to. This allows an attacker to replay a request to any number of OCSP responders. [RFC 2560: 2.1, 5]
An OCSP request may contain optional extensions.	O	[RFC 2560: 2.1, 4.1.2]
The critical flag should not be set for any of them.	O/R	[RFC 2560: 4.1.2]
The requestor may choose to sign the OCSP request.	O	[RFC 2560: 4.1.2]
For signature calculation, the data to be signed is encoded using the ASN.1] distinguished encoding rules (DER) [X.690].	m	[RFC 2560: 4]
The signature is computed over the tbsRequest structure.	m	[RFC 2560: 4.1.2]
The requestor shall specify its name in the requestorName field.	m	[RFC 2560: 4.1.2]
The requestor may include certificates that help the OCSP responder verify the requestor's signature in the certs field of Signature.	o	[RFC 2560: 4.1.2]
Formatting of the request message could vary depending on the transport mechanism used (HTTP, SMTP, LDAP, etc.).	O	Implementers are advised to consider the reliability of HTTP cache mechanisms when deploying OCSP over HTTP. [RFC 2560: 4.1, 5]
The serviceLocator request extension may be included as one of the singleRequestExtensions in requests.	O	id-pkix-ocsp-service-locator OID ::= { id-pkix-ocsp 7 } [RFC 2560: 4.4.6]
Values for the issuer and locator fields are obtained from the corresponding fields in the subject certificate.		[RFC 2560: 4.4.6]

OCSP Responder		
Upon receipt of request the OCSP Responder determines if: 1. the message is well formed 2. the responder can provide requested service 3. the request contains the needed information	M	[RFC 2560: 2.1]

Protocol Action	Status	Notes
If one of the conditions is not meet, the OCSP Responder returns an error message.	M	[RFC 2560: 2.1, 2.3]
If the conditions are met, the OCSP Responder returns a message containing requested service.	M	[RFC 2560: 2.1]
Upon receipt of request, the OCSP Responder may process requested extensions.	O	[RFC 2560: 2.1]
Unrecognized, non-critical extensions must be ignored	m	[RFC 2560: 4.1.2]
Unrecognized, critical extensions must be handled by an exception routine.	m	[RFC 2560: 4.1.2]
The key used to sign the response must belong to one of the following: 1. the CA who issued the certificate in question 2. a Trusted Responder whose public key is trusted by the requester 3. a CA Designated Responder (Authorized Responder)	M	[RFC 2560: 2.2, 4.2.2.2]
OCSP responders shall be capable of producing responses of the id-pkix-ocsp-basic response type.	M	[RFC 2560: 2.2, 4.2.1, 4.4.3]
OCSP responders may pre-produce signed responses specifying the status of certificates at a specified time.	O	The use of pre-produce responses allows replay attacks. [RFC 2560: 2.5, 5]
The time at which the status was known to be correct shall be reflected in the thisUpdate field of the response.	m	[RFC 2560: 2.5]
The time at or before which newer information will be available is reflected in the nextUpdate field.	m	[RFC 2560: 2.5]
The time at which the response was produced will appear in the producedAt field of the response.	m	[RFC 2560: 2.5]
A certificate's issuer may delegates OCSP signing authority.	O	[RFC 2560: 2.6]
An Authorized OCSP Responder must have a certificate containing a unique value for extendedKeyUsage.	m	[RFC 2560: 2.6, 4.2.2.2]
An Authorized Responder must receive this certificate directly from the delegating CA.	m	[RFC 2560: 2.6]
If an OCSP responder knows that a particular CA's private key has been compromised, it MAY return the revoked state for all certificates issued by that CA.	O	[RFC 2560: 2.7]
An Authorized OCSP responder may provide status information for one or more CAs.	O	[RFC 2560: 4.2.2.2.1]
OCSP responders shall support the SHA1 hashing algorithm.	M	[RFC 2560: 4.3]
The OCSP responder may support nonce cryptographic binding a request and a response by including OID id-pkix-ocsp-nonce as one of the responseExtensions.	O	id-pkix-ocsp-nonce OID ::= { id-pkix-ocsp 2 } [RFC 2560: 4.4.1]
The OCSP responder may indicate the CRL on which a revoked or onHold certificate is found.	O	[RFC 2560: 4.4.2]
The CRL may be specified by a URL where it is available.	o	[RFC 2560: 4.4.2]
The CRL may be specified by its CRL number.	o	[RFC 2560: 4.4.2]
The CRL may be specified by the time at which the relevant CRL was created.	o	[RFC 2560: 4.4.2]
These extensions will be specified as response singleExtensions.	m	[RFC 2560: 4.4.2]

Protocol Action	Status	Notes
The identifier for this extension will be id-pkix-ocsp-crl, while the value will be CrIID.	m	id-pkix-ocsp-crl [RFC 2560: 4.4.2]      OID ::= { id-pkix-ocsp 3 }
An OCSP responder may choose to retain revocation information beyond a certificate's expiration.	O	[RFC 2560: 4.4.4]
The archive cutoff date is determined by subtracting the retention interval value from the producedAt time.	m	[RFC 2560: 4.4.4]
In order to support such historical reference an archive cutoff date extension should be include in responses.	o	[RFC 2560: 4.4.4]
If included, this value shall be provided as an OCSP singleExtensions extension identified by id-pkix-ocsp-archive-cutoff and of syntax GeneralizedTime.	m	id-pkix-ocsp-archive-cutoff [RFC 2560: 4.4.4]      OID ::= { id-pkix-ocsp 6 }
An OCSP server may upon receiving a request route it to the OCSP server, which is known to be authoritative for the identified certificate.	M	[RFC 2560: 4.4.6]

OCSP Response		
OCSP response consists of response type and data.	M	[RFC 2560: 2.2]
All non-error response messages must be digitally signed.	M	[RFC 2560: 2.2]
A response message is composed of: <ul style="list-style-type: none"> <li>1. version of the response syntax</li> <li>2. name of the responder</li> <li>3. responses for each of the certificates in a request</li> <li>4. optional extensions</li> <li>5. signature algorithm OID</li> <li>6. signature computed across hash of the response</li> </ul>	M	[RFC 2560: 2.2]
The response for each of the certificates in a request consists of: <ul style="list-style-type: none"> <li>1. target certificate identifier</li> <li>2. certificate status value</li> <li>3. response validity interval</li> </ul>	M	[RFC 2560: 2.2]
The response for each of the certificates in a request may include optional extensions.	O	[RFC 2560: 2.2]
One of the following definitive response indicators is used in the certificate status value: <ul style="list-style-type: none"> <li>1. good - indicates that the certificate is not revoked</li> <li>2. revoked - indicates that the certificate has been revoked (either permanently or temporarily (on hold))</li> <li>3. unknown - indicates that the responder doesn't know about the certificate being requested.</li> </ul>	M	[RFC 2560: 2.2]
OCSP Responder error messages are not digitally signed.	M	[RFC 2560: 2.3]

Protocol Action	Status	Notes
<p>Errors can be of the following types:</p> <ol style="list-style-type: none"> <li>malformedRequest - if the request received does not conform to the OCSP syntax</li> <li>internalError - indicates that the OCSP responder reached an inconsistent internal state</li> <li>tryLater - indicates that the service exists, but is temporarily unable to respond</li> <li>sigRequired - indicates that the requestor did not sign the request</li> <li>unauthorized - the requestor is not authorized to make this query to this server</li> </ol>	O	[RFC 2560: 2.3]
<p>Responses can contain three times in them:</p> <ol style="list-style-type: none"> <li>thisUpdate - the time at which the status being indicated was known to be correct</li> <li>nextUpdate - the time at or before which newer information will be available about the status of the certificate</li> <li>producedAt - the time at which the OCSP responder signed this response.</li> </ol>	O	[RFC 2560: 2.4]
If nextUpdate is not set, the responder must have newer revocation information available all the time.	m	[RFC 2560: 2.4, 4.2.2.1]
The validity interval defined by thisUpdate and nextUpdate must correspond to the interval in CRLs.	m	[RFC 2560: 4.2.2.1]
For signature calculation, the data to be signed is encoded using the ASN.1 distinguished encoding rules (DER) [X.690].	M	[RFC 2560: 4]
Formatting of the response message could vary depending on the transport mechanism used (HTTP, SMTP, LDAP, etc.).	O	Implementers are advised to consider the reliability of HTTP cache mechanisms when deploying OCSP over HTTP. [RFC 2560: 4.2, 5]
An OCSP response at a minimum consists of a responseStatus field indicating the processing status of the prior request.	M	[RFC 2560: 4.2.1]
If responseStatus is one of the error conditions, responseBytes are not set.	M	[RFC 2560: 4.2.1]
The value for response shall be the DER encoding of BasicOCSPResponse.	M	[RFC 2560: 4.2.1]
The value for BasicOCSPResponse signature shall be computed on the hash of the DER encoding ResponseData.	M	[RFC 2560: 4.2.1]
The CRL Entry Extensions are supported as singleExtensions.	M	[RFC2459: 5.3; RFC 2560: 4.4.5]

### Status Notation:

M = Mandatory in all implementations  
m = Mandatory if an option is exercised  
O = Optional  
O/R = Optional but recommended  
o = Optional if an option is exercised  
o/r = Optional if an option is exercised but recommended  
I = Implemented option  
NO = Option not used in this implementation  
N/A = Does not apply to this implementation

### Message Syntax

Message Field	Value	Comment
OCSPRequest	SEQUENCE	
tbsRequest		
TBSRequest	SEQUENCE	
version [0]	EXPLICIT	DEFAULT v1. MANDATORY
Version	INTEGER	v1(0)
requestorName [1]	EXPLICIT	OPTIONAL
GeneralName	CHOICE	[RFC 2459: A.2]
otherName [0]		
AnotherName	SEQUENCE	AnotherName replaces OTHER-NAME ::= TYPE-IDENTIFIER, as TYPE-IDENTIFIER is not supported in the '88 ASN.1 syntax
type-id	OBJECT IDENTIFIER	
value [0]	EXPLICIT ANY DEFINED BY type-id	
rfc822Name [1]	IA5String	
dNSName [2]	IA5String	
x400Address [3]		x400 address syntax starts here OR Names
ORAddress	SEQUENCE	[RFC 2459: A.1]
built-in-standard-attributes		
BuiltInStandardAttributes	SEQUENCE	Built-in Standard Attributes.

Message Field	Value	Comment
country-name		OPTIONAL.
CountryName	[APPLICATION 1] CHOICE	
x121-dcc-code	NumericString	(SIZE (ub-country-name-numeric-length))
iso-3166-alpha2-code	PrintableString	(SIZE (ub-country-name-alpha-length))
administration-domain-name	AdministrationDomainName	OPTIONAL.
network-address [0]		OPTIONAL. See also extended-network-address.
NetworkAddress		
X121Address	NumericString	(SIZE (1..ub-x121-address-length))
terminal-identifier [1]		OPTIONAL.
TerminalIdentifier	PrintableString	(SIZE (1..ub-terminal-id-length))
private-domain-name [2]		OPTIONAL.
PrivateDomainName	CHOICE	
numeric	NumericString	(SIZE (1..ub-domain-name-length))
printable	PrintableString	(SIZE (1..ub-domain-name-length))
organization-name [3]		OPTIONAL. See also teletex-organization-name.
OrganizationName	PrintableString	(SIZE (1..ub-organization-name-length))
numeric-user-identifier [4]		OPTIONAL.
NumericUserIdentifier	NumericString	(SIZE (1..ub-numeric-user-id-length))
personal-name [5]		OPTIONAL. See also teletex-personal-name.
PersonalName	SET	
surname [0]	PrintableString	(SIZE (1..ub-surname-length))
given-name [1]	PrintableString	OPTIONAL. (SIZE (1..ub-given-name-length))
initials [2]	PrintableString	OPTIONAL. (SIZE (1..ub-initials-length))
generation-qualifier [3]	PrintableString	OPTIONAL. (SIZE (1..ub-generation-qualifier-length))
organizational-unit-names [6]		OPTIONAL. See also teletex-organizational-unit-names.
OrganizationalUnitNames	SEQUENCE SIZE (1..ub-organizational-units) OF	
OrganizationalUnitName	PrintableString	(SIZE (1..ub-organizational-unit-name-length))
built-in-domain-defined-attributes		OPTIONAL. Built-in Domain-defined Attributes. See also teletex-domain-defined-attributes.
BuiltInDomainDefinedAttributes	SEQUENCE SIZE (1..ub-domain-defined-attributes) OF	
BuiltInDomainDefinedAttribute	SEQUENCE	
type	PrintableString	(SIZE (1..ub-domain-defined-attribute-type-length))
value	PrintableString	(SIZE (1..ub-domain-defined-attribute-value-length))

Message Field	Value	Comment
extension-attributes		OPTIONAL. The OR-address is semantically absent from the OR-name if the built-in-standard-attribute sequence is empty and the built-in-domain-defined-attributes and extension-attributes are both omitted.
ExtensionAttributes	SET SIZE (1..ub-extension-attributes) OF	
ExtensionAttribute	SEQUENCE	
extension-attribute-type [0]	INTEGER	(0..ub-extension-attributes)
extension-attribute-value [1]		ANY DEFINED BY extension-attribute-type
directoryName [4]		
Name	CHOICE	Only one possibility for now. [RFC 2459: A.1]
rdnSequence		
RDNSequence	SEQUENCE OF	
RelativeDistinguishedName	SET SIZE (1 .. MAX) OF	
AttributeTypeAndValue		Arc for standard naming attributes id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
type		
AttributeType	OBJECT IDENTIFIER	
{id-at 41} {id-at 4} {id-at 42} {id-at 43} {id-at 44}		id-at-name id-at-surname id-at-givenName id-at-initials id-at-generationQualifier
X520name	CHOICE	
teletexString	TeletexString	(SIZE (1..ub-name))
printableString	PrintableString	(SIZE (1..ub-name))
universalString	UniversalString	(SIZE (1..ub-name))
utf8String	UTF8String	(SIZE (1..ub-name))
bmpString	BMPString	(SIZE(1..ub-name))
{id-at 3}	X520CommonName	id-at-commonName
{id-at 7}	X520LocalityName	id-at-localityName
{id-at 8}	X520StateOrProvinceName	id-at-stateOrProvinceName
{id-at 10}	X520OrganizationName	id-at-organizationName
{id-at 11}	X520OrganizationalUnitName	id-at-organizationalUnitName
{id-at 12}	X520Title	id-at-title
{id-at 46}		id-at-dnQualifier

Message Field	Value	Comment
X520dnQualifier	PrintableString	
{id-at 6}		id-at-countryName
X520countryName	PrintableString (SIZE (2))	IS 3166 codes
emailAddress		Legacy attribute.
{ pkcs-9 1 }	1 2 840 113549 1 9	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }
Pkcs9email	IA5String	(SIZE (1..ub-emailaddress-length))
value		
AttributeValue	ANY	
ediPartyName [5]		
EDIPartyName	SEQUENCE	
nameAssigner [0]		OPTIONAL.
DirectoryString	CHOICE	[RFC 2459: A.1]
teletexString	TeletexString (SIZE (1..MAX))	
printableString	PrintableString (SIZE (1..MAX))	
universalString	(SIZE (1..MAX))	
UniversalString	[UNIVERSAL 28] IMPLICIT OCTET STRING	UniversalString is defined in ASN.1:1993. [RFC 2459: A.1]
utf8String	(SIZE (1..MAX))	
UTF8String	[UNIVERSAL 12] IMPLICIT OCTET STRING	The content of this type conforms to RFC 2279.
bmpString	(SIZE(1..MAX))	
BMPString	[UNIVERSAL 30] IMPLICIT OCTET STRING	BMPString is the subtype of UniversalString and models the Basic Multilingual Plane of ISO/IEC/ITU 10646-1. [RFC 2459: A.1]
partyName [1]	DirectoryString	
uniformResourceIdentifier [6]	IA5String	
iPAddress [7]	OCTET STRING	
registeredID [8]	OBJECT IDENTIFIER	
requestList	SEQUENCE OF	
Request	SEQUENCE	
reqCert		MANDATORY
CertID	SEQUENCE	
hashAlgorithm		[RFC 2560: 4.1.1]

Message Field	Value	Comment
AlgorithmIdentifier	SEQUENCE	[RFC 2459: 4.1.1.2, A.1]
algorithm	OID	
parameters		OPTIONAL. ANY DEFINED BY algorithm.
issuerNameHash	OCTET STRING	Hash calculated over the DER encoding of the issuer's name field in the certificate being checked. [RFC 2560: 4.1.1, 4.1.2]
issuerKeyHash	OCTET STRING	Hash calculated over the value (excluding tag and length) of the subject public key field in the issuer's certificate. [RFC 2560: 4.1.1, 4.1.2]
serialNumber		The serial number of the certificate for which status is being requested. [RFC 2560: 4.1.1]
CertificateSerialNumber	INTEGER	[RFC 2459: 4.1, 4.1.2.2]
singleRequestExtensions [0]	EXPLICIT	OPTIONAL
Extensions	SEQUENCE SIZE (1..MAX) OF	[RFC 2459: 4.1, 4.1.2.9, A.1]
Extension	SEQUENCE	
extnID	OBJECT IDENTIFIER	id-pkix-ocsp-nonce      OID ::= { id-pkix-ocsp 2 } id-pkix-ocsp-service-locator      OID ::= { id-pkix-ocsp 7 }
critical	BOOLEAN	DEFAULT FALSE
extnValue	OCTET STRING	
Nonce	value	
ServiceLocator	SEQUENCE	
issuer	Name	
locator		id-pe-authorityInfoAccess      OID ::= { id-pe 1 }
AuthorityInfoAccessSyntax	SEQUENCE SIZE (1..MAX) OF	Only certificates that can be checked by OCSP can have this extension. [RFC 2560: 3.1, RFC 2459: 4.2.2.1]
AccessDescription	SEQUENCE	
accessMethod	OBJECT IDENTIFIER	
accessLocation	GeneralName	Defines the transport used to access the OCSP responder.
requestExtensions [2]	EXPLICIT Extensions	OPTIONAL

Message Field	Value	Comment
AcceptableResponses	SEQUENCE OF OBJECT IDENTIFIER	id-kp-OCSPSigning      OID ::= { id-kp 9 } id-pkix-ocsp            OID ::= { id-ad-ocsp } id-pkix-ocsp-basic      OID ::= { id-pkix-ocsp 1 } id-pkix-ocsp-nonce      OID ::= { id-pkix-ocsp 2 } id-pkix-ocsp-crl        OID ::= { id-pkix-ocsp 3 } [RFC 2560: 4.4.2] id-pkix-ocsp-response    OID ::= { id-pkix-ocsp 4 } id-pkix-ocsp-nocheck    OID ::= { id-pkix-ocsp 5 } [RFC 2560: 4.2.2.2.1] id-pkix-ocsp-archive-cutoff    OID ::= { id-pkix-ocsp 6 } id-pkix-ocsp-service-locator    OID ::= { id-pkix-ocsp 7 }
optionalSignature [0]	EXPLICIT	OPTIONAL
Signature	SEQUENCE	
signatureAlgorithm	AlgorithmIdentifier	
signature	BIT STRING	
certs [0]	EXPLICIT SEQUENCE OF Certificate	OPTIONAL

OCSPResponse	SEQUENCE	
responseStatus		MANDATORY [RFC 2560: 4.2.1]
OCSPResponseStatus	ENUMERATED	(4) is not used. [RFC 2560: 2.3]
successful (0)		Response has valid confirmations
malformedRequest (1)		Illegal confirmation request
internalError (2)		Internal error in issuer
tryLater (3)		Try again later
sigRequired (5)		Must sign the request
unauthorized (6)		Request unauthorized
responseBytes [0]	EXPLICIT	OPTIONAL. If the value of responseStatus is one of the error conditions, responseBytes are not set. [RFC 2560: 4.2.1]
ResponseBytes	SEQUENCE	
responseType	OBJECT IDENTIFIER	Must support: id-pkix-ocsp      OID ::= { id-ad-ocsp } id-pkix-ocsp-basic    OID ::= { id-pkix-ocsp 1 }
response	OCTET STRING	The DER encoding of BasicOCSPResponse.

Message Field	Value	Comment
BasicOCSPResponse	SEQUENCE	
tbsResponseData		
ResponseData	SEQUENCE	
version [0]	EXPLICIT Version	DEFAULT v1. MANDATORY.
responderID		MANDATORY
ResponderID	CHOICE	
byName [1]	Name	
byKey [2]		<p>The key used to sign the response MUST belong to one of the following:</p> <ol style="list-style-type: none"> <li>1. the CA who issued the certificate in question</li> <li>2. a Trusted Responder whose public key is trusted by the requester</li> <li>3. a CA Designated Responder (Authorized Responder) who holds a specially marked certificate issued directly by the CA, indicating that the responder may issue OCSP responses for that CA [RFC 2560: 2.2]</li> </ol>
KeyHash	OCTET STRING	SHA-1 hash of responder's public key (excluding the tag and length fields).
producedAt		The time at which the OCSP responder signed this response. [RFC 2560: 2.4]
GeneralizedTime	YYYYMMDDHHMMSSZ	[RFC 2459: 4.1.2.5.2]
responses	SEQUENCE OF	MANDATORY
SingleResponse	SEQUENCE	
certID	CertID	MANDATORY
certStatus		MANDATORY
CertStatus	CHOICE	
good [0]	IMPLICIT NULL	<p>A positive response indicating that the certificate is not revoked. Does not necessarily mean that the certificate was ever issued, or that at the response time the certificate was still valid. Response extensions may be used to convey additional information [RFC 2560: 2.2]</p>
revoked [1]	IMPLICIT	<p>The certificate has been revoked (either permanantly or temporarily (on hold)). [RFC 2560: 2.2]</p>
RevokedInfo	SEQUENCE	

Message Field	Value	Comment
revocationTime	GeneralizedTime	
revocationReason [0]	EXPLICIT	OPTIONAL
CRLReason	ENUMERATED	X.509: 12.5.2.2
unspecified (0)		
keyCompromise (1)		
cACompromise (2)		Responder MAY return revoked state for all certificates issued by a compromised CA. [RFC 2560: 2.7]
affiliationChanged (3)		
superseded (4)		
cessationOfOperation (5)		
certificateHold (6)		
removeFromCRL (8)		
unknown [2]	IMPLICIT	Indicates that the responder doesn't know about the certificate being requested. [RFC 2560: 2.2]
UnknownInfo	NULL	This can be replaced with an enumeration.
thisUpdate	GeneralizedTime	The time at which the status being indicated is known to be correct. [RFC 2560: 2.4]
nextUpdate [0]	EXPLICIT GeneralizedTime	OPTIONAL. The time at or before which newer information will be available about the status of the certificate. [RFC 2560: 2.4]
singleExtensions [1]	EXPLICIT Extensions	OPTIONAL
CrlID	SEQUENCE	id-pkix-ocsp-crl [RFC 2560:4.4.2]      OID ::= { id-pkix-ocsp 3 }
crlUrl [0]	EXPLICIT IA5String	OPTIONAL. The URL at which the CRL is available.
crlNum [1]	EXPLICIT INTEGER	OPTIONAL. The value of the CRL number extension of the relevant CRL.
crlTime [2]	EXPLICIT GeneralizedTime	OPTIONAL. The time at which the relevant CRL was issued.
ArchiveCutoff	GeneralizedTime	id-pkix-ocsp-archive-cutoff      OID ::= { id-pkix-ocsp 6 } [RFC 2560:4.4.4]
CRLReason	ENUMERATED	id-ce-cRLReason      OID ::= { id-ce 21 } [RFC 2459: 5.3.1]

Message Field	Value	Comment
holdInstructionCode	OBJECT IDENTIFIER	id-ce-holdInstructionCode      OID ::= { id-ce 23 } holdInstruction                OID ::= { iso(1) member- body(2) us(840) x9-57(10040) 2 } id-holdinstruction-none        OID ::= {holdInstruction 1} id-holdinstruction-callissuer    OID ::= {holdInstruction 2} id-holdinstruction-reject        OID ::= {holdInstruction 3} [RFC 2459: 5.3.2]
invalidityDate	GeneralizedTime	ZULU Time id-ce-invalidityDate            OID ::= { id-ce 24 } [RFC 2459: 5.3.3]
certificateIssuer	GeneralNames	id-ce-certificateIssuer        OID ::= { id-ce 29 } [RFC 2459: 5.3.4]
responseExtensions [1]	EXPLICIT Extensions	OPTIONAL id-pkix-ocsp-nonce              OID ::= { id-pkix-ocsp 2 }
signatureAlgorithm	AlgorithmIdentifier	MANDATORY. [RFC 2560:4.3; RFC 2459:7.2.1, 7.2.2]
signature	BIT STRING	MANDATORY. The value for signature shall be computed on the hash of the DER encoding ResponseData. [RFC 2560: 2.2, 4.2.1]
certs [0]	EXPLICIT SEQUENCE OF Certificate	OPTIONAL